

Inhalt

Einleitung	19
1 Einführung in SAP HANA	23
1.1 Der technische Aufbau von SAP HANA	24
1.1.1 Zeilen- und spaltenorientierte Tabellen	24
1.1.2 Der Systemtyp einer SAP-HANA-Datenbank	26
1.1.3 Schemata	26
1.1.4 Zugriff auf Daten in der SAP-HANA-Datenbank	31
1.2 SAP HANA Cockpit	31
1.2.1 Ressource-Gruppen	33
1.2.2 Benutzerverwaltung im SAP HANA Cockpit	34
1.2.3 Ressourcen ins SAP HANA Cockpit einbinden	37
1.2.4 Templates für die Systemkonfiguration	39
1.2.5 Verwaltung von SAP-HANA-Datenbanken	42
1.3 SAP HANA Database Explorer	46
1.3.1 Die Oberfläche des SAP HANA Database Explorer	47
1.3.2 Der SQL-Editor	48
1.3.3 Die SQL Statement Library	49
1.4 SAP HANA Studio	52
1.4.1 Die Oberfläche von SAP HANA Studio	53
1.4.2 Suche und Anzeige von Tabellen und Views	57
1.4.3 Anlegen neuer Remote Sources	59
1.4.4 Ausführen von SQL-Statements	59
1.4.5 Das Repository der SAP-HANA-Datenbank	61
1.5 HDBSQL	64
1.5.1 Skript-gesteuerte Nutzung von hdbsql	67
1.5.2 Ausgabe von Befehlen in eine Textdatei	68
1.6 DBA Cockpit	68
1.7 SAP HANA XS ADVANCED	72
1.7.1 Zugriff auf SAP HANA XSA	72
1.7.2 Struktur in SAP HANA XSA	73
1.7.3 SAP HANA XSA Cockpit	74
1.7.4 SAP WebIDE	76

1.8	SAP HANA und SAP ERP bzw. SAP S/4HANA	77
1.9	Leitfäden zur SAP-HANA-Sicherheit	80

2 Netzwerk- und Betriebssystemsicherheit 85

2.1	Absicherung der UNIX-Benutzer	85
2.1.1	Speicherung der UNIX-Benutzer	85
2.1.2	Benutzer <sid>adm	87
2.1.3	Benutzer sapadm	88
2.1.4	Benutzer des SAP HANA XS Advanced	88
2.1.5	Benutzer root	89
2.1.6	Gruppe sapsys	89
2.1.7	Sperrungen von Benutzeranmeldungen unter UNIX	90
2.2	Schutz von Dateien und Verzeichnissen	91
2.2.1	Datei- und Verzeichnisrechte	91
2.2.2	Die Datei .bash_history	92
2.2.3	Schutz von exportierten Dateien	94
2.3	Zugriff auf die UNIX-Ebene vom ABAP-Stack aus	94
2.3.1	Funktionsweise	95
2.3.2	Der Report RSBDCOS0	98
2.3.3	Berechtigungen für Betriebssystemkommandos	99
2.4	Protokollierung von Aktionen unter UNIX	100

3 Systemsicherheit in SAP HANA 103

3.1	Verwaltung von Lizenzen	103
3.1.1	Auswertung der aktuellen Lizenzen	104
3.1.2	Lizenzen mit dem SAP HANA Cockpit verwalten	106
3.1.3	Lizenzen mit dem SAP HANA Studio verwalten	107
3.1.4	Protokollierung von Änderungen an Lizenzen	107
3.2	Pflege von Systemparametern	108
3.2.1	Das Konzept der Systemparameter	108
3.2.2	Ändern der Parameter mit dem SAP HANA Cockpit	112
3.2.3	Ändern der Parameter mit dem SAP HANA Studio	116

3.2.4	Ändern der Parameter mit SQL-Statements	118
3.2.5	Änderungshistorie von Parameteränderungen	119
3.3	Verschlüsselung von Daten	122
3.3.1	Secure Store in the File System (SSFS)	122
3.3.2	Berechtigungen zur Pflege der Einstellungen zur Verschlüsselung	125
3.3.3	Initiale Verschlüsselung bei Anlegen von Datenbanken	126
3.3.4	Verschlüsselung der persistenten Daten	127
3.3.5	Verschlüsselung der Redo-Logs	131
3.3.6	Verschlüsselung der Backups	132
3.3.7	Backup der Root Keys	133
3.3.8	Protokollierung von Änderungen an der Verschlüsselung	134
3.3.9	Client-Side Data Encryption	136
3.4	Verschlüsselung der Kommunikation	139
3.4.1	Analyse der Einstellungen zur Verschlüsselung	139
3.4.2	Mitlesen von Daten	140
3.5	Verbindungen zu anderen Systemen – Remote Sources	143
3.5.1	Eigenschaften von Remote Sources	143
3.5.2	Secondary Credentials	146
3.5.3	Berechtigungen für Remote Sources	147
3.5.4	Pflege von Remote Sources mit dem SAP HANA Database Explorer	148
3.5.5	Pflege von Remote Sources mit dem SAP HANA Studio	153
3.5.6	Pflege von Remote Sources mittels SQL-Statements	155
3.5.7	Zugriff auf Daten in der Remote Source	155
3.5.8	Protokollierung von Remote Sources	157
3.6	Skripte zur Prüfung der Systemsicherheit	158
3.6.1	Das Skript HANA_Security_MiniChecks	158
3.6.2	Das Skript HANA_Configuration_MiniChecks	160
3.7	Alerts	163
3.7.1	Statistics Service	163
3.7.2	Sicherheitsrelevante Alarmmeldungen	164
3.7.3	Auswertung und Konfiguration von Alarmmeldungen mit dem SAP HANA Cockpit	168
3.7.4	Auswertung und Konfiguration von Alarmmeldungen mit dem SAP HANA Studio	169
3.7.5	Definition von Schwellwerten	170
3.7.6	Berechtigungen zur Auswertung von Alerts	172

4	Sicherheit in Multi-Tenant-Datenbanken	173
4.1	Das Konzept der Tenant-Datenbanken	173
4.1.1	Berechtigungen zur Verwaltung von Tenants	176
4.1.2	Verwaltung von Tenants mit dem SAP HANA Cockpit	177
4.1.3	Verwaltung von Tenants mit SAP HANA XSA	179
4.2	Tenant-übergreifende Zugriffe	181
4.3	Nicht änderbare Parameter in Tenants	181
4.4	Einschränkung von Funktionen in Tenants	182
4.5	High Isolation Level für Tenants	184
4.6	Protokollierung von Änderungen an Tenants	189
5	Authentifizierung in SAP HANA	191
5.1	Authentifizierungsmethoden	191
5.1.1	Konfiguration der möglichen Authentifizierungsmethoden	191
5.1.2	Kennwortbasierte Anmeldung	192
5.1.3	Anmeldung mittels Kerberos-Authentifizierung	192
5.1.4	Anmeldung mittels SAP Logon Ticket	194
5.1.5	Anmeldung mittels Security Assertion Markup Language (SAML)	194
5.1.6	Anmeldung mittels X.509-Zertifikat	195
5.1.7	Anmeldung mittels JSON Web Token	195
5.1.8	Authentifizierungsmethoden setzen mit dem SAP HANA Cockpit	195
5.1.9	Authentifizierungsmethoden setzen mit dem SAP HANA Studio	197
5.1.10	Authentifizierungsmethoden setzen mit SQL-Statements	199
5.1.11	Auswertung der zugeordneten Authentifizierungsmethoden	200
5.1.12	Protokollierung der Authentifizierung	202
5.2	Kennwortrichtlinien	204
5.2.1	Systemparameter für Kennwortrichtlinien	204
5.2.2	Benutzergruppenspezifische Kennwortrichtlinien	211
5.2.3	Liste der verbotenen Kennwörter	212
5.2.4	Pflege der Richtlinien mit dem SAP HANA Cockpit	213
5.2.5	Pflege der Richtlinien mit dem SAP HANA Studio	214
5.2.6	Pflege der Richtlinien mit SQL-Statements	215
5.2.7	Analyse der Kennwortrichtlinien	217
5.2.8	Protokollierung der Änderung an den Kennwortrichtlinien	217

6 Benutzerverwaltung in SAP HANA 221

6.1	Der Benutzerstammsatz	221
6.1.1	Eigenschaften eines Benutzerstammsatzes	222
6.1.2	Restricted User	227
6.1.3	Temporäre Sperrung aller Nicht-Admin-Benutzer	229
6.1.4	Berechtigungen	230
6.1.5	Benutzerpflege mit dem SAP HANA Cockpit	230
6.1.6	Benutzerpflege mit dem SAP HANA Studio	235
6.1.7	Benutzerpflege per SQL	236
6.1.8	Kopieren von Benutzern und Berechtigungen	240
6.1.9	Protokollierung der Benutzerverwaltung	243
6.2	SAP-HANA-XS-Advanced-Benutzer	244
6.2.1	Eigenschaften der SAP-HANA-XSA-Benutzer	244
6.2.2	Anlegen neuer Benutzer in SAP HANA XSA	247
6.2.3	Migrieren eines Datenbankbenutzers nach SAP HANA XSA	249
6.2.4	Protokollierung von Änderungen an SAP-HANA-XSA-Benutzern	250
6.3	SAP-HANA-Standardbenutzer	251
6.3.1	Der Benutzer SYSTEM	252
6.3.2	Systembenutzer	253
6.3.3	Benutzer des SAP HANA XS Advanced	254
6.3.4	Benutzer der SAP HANA Deployment Infrastructure (HDI)	255
6.3.5	Der Benutzer SAP<sid>	255
6.4	Remote-Benutzer	257
6.5	Benutzergruppen	261
6.5.1	Pflege von Benutzergruppen mit dem SAP HANA Cockpit	261
6.5.2	Pflege von Benutzergruppen mit SQL	263
6.5.3	Protokollierung von Benutzergruppen	265

7 Das Berechtigungskonzept von SAP HANA 267

7.1	Konzept der SAP-HANA-Berechtigungen	267
7.2	System Privileges	269
7.2.1	Kategorisierung der System Privileges	270
7.2.2	Zuordnung von System Privileges	278
7.3	Object Privileges	282
7.3.1	Object Privileges für Katalogobjekte	284

7.3.2	Object Privileges auf die Daten des SAP-ERP- bzw. SAP-S/4HANA-Systems	289
7.3.3	Zuordnung von Object Privileges	289
7.4	Package Privileges	293
7.4.1	Kritische Package Privileges	296
7.4.2	Zuordnung von Package Privileges	296
7.5	Analytic Privileges	300
7.6	Application Privileges	300
7.6.1	Application Privileges in Repository-Rollen	302
7.6.2	Application Privileges in Katalogrollen	302
7.6.3	Direkte Zuordnung von Application Privileges zu Benutzern	303
7.6.4	Zuordnung von Application Privileges über Prozeduren	305
7.7	Weitergabe von Berechtigungen	305
7.8	Maskierung von Daten	307
7.9	Privileges on Users	309
7.10	Kopieren von Berechtigungen	310
7.11	Trace von Berechtigungen	312
7.11.1	Die Trace-Konfiguration	313
7.11.2	Berechtigungs-Trace für alle Benutzer	314
7.11.3	Berechtigungs-Trace für einzelne Benutzer	315
7.11.4	Auswertung des Berechtigungs-Trace	316
7.11.5	Aktivierung und Auswertung des Trace mit dem SAP HANA Cockpit	317
7.11.6	Aktivierung und Auswertung des Trace mit dem SAP HANA Studio	320
7.12	Berechtigungen in SAP HANA XS Advanced	323
7.12.1	Role Collections	324
7.12.2	Scopes und Attributes	326
7.12.3	Rollen-Templates und Rollen	328
7.12.4	Berechtigungen auf Organizations und Spaces	329
8	Das Rollenkonzept von SAP HANA	333
8.1	Eigenschaften von Rollen	333
8.1.1	Speicherung von Rollen	334
8.1.2	Namenskonventionen für Rollen	335

8.2	Runtime-Katalogrollen	339
8.2.1	Weitergabe zugeordneter Rollen	340
8.2.2	Pflege von Katalogrollen mit dem SAP HANA Cockpit	341
8.2.3	Pflege von Katalogrollen mit dem SAP HANA Studio	344
8.2.4	Pflege von Katalogrollen mit SQL	345
8.2.5	Änderungshistorie von Katalogrollen	347
8.3	Design-Time-Repository-Rollen (XSC)	348
8.3.1	Pflege von Repository-Rollen mit dem SAP HANA Studio	349
8.3.2	Pflege von Repository-Rollen mit dem SAP HANA Cockpit	357
8.3.3	Repository-Rollen Benutzern zuordnen	358
8.3.4	Änderungshistorie von Repository-Rollen	359
8.4	Design-Time-HANA-DI-Rollen (XSA)	360
8.4.1	Pflege von HDI-Containern mit SAP WebIDE	361
8.4.2	Pflege von HDI-Rollen in der WebIDE	362
8.4.3	HDI-Rollen Benutzern zuordnen	365
8.4.4	Änderungshistorie von HDI-Rollen	367
8.5	SAP-HANA-Standardrollen	367
8.5.1	Die Rolle PUBLIC	367
8.5.2	Die Rolle SAP_INTERNAL_HANA_SUPPORT	369
8.5.3	Die Rolle CONTENT_ADMIN	370
8.5.4	Die Rolle MODELING	370
8.5.5	Die Rolle MONITORING	370
9	Analyse des SAP-HANA-Berechtigungskonzepts	371
<hr/>		
9.1	Tabellen und Views zur Analyse von Berechtigungen	371
9.2	Analysen aus Benutzersicht	373
9.2.1	Wurden Berechtigungen direkt in den Benutzerstammsatz eingetragen?	373
9.2.2	Welche Rollen wurden den Benutzern zugeordnet?	375
9.2.3	Wurden Benutzern Repository-Rollen zugeordnet?	375
9.2.4	Welche Katalogrollen wurden Benutzern zugeordnet?	376
9.3	Analysen aus Berechtigungssicht	377
9.4	Auswertung effektiver Berechtigungen	379
9.4.1	Die View ACCESSIBLE_VIEWS	380
9.4.2	Die View EFFECTIVE_PRIVILEGES	381
9.4.3	Die View EFFECTIVE_PRIVILEGE_GRANTEES	383

9.4.4	Die View EFFECTIVE_ROLES	386
9.4.5	Die View EFFECTIVE_ROLE_GRANTEES	386
9.4.6	Die View EFFECTIVE_APPLICATION_PRIVILEGES	387
9.5	Das Skript HANA_Security_GrantedRolesAndPrivileges	388
9.6	Praktische Beispiele für Berechtigungsanalysen	390
9.6.1	Berechtigungen zur Benutzer- und Berechtigungsverwaltung	390
9.6.2	Berechtigungen zur Systemadministration	392
9.6.3	Berechtigungen zur Anwendungsentwicklung	393
9.6.4	Berechtigungen für Datenzugriffe	395
9.6.5	Funktionstrennungen	396
10	Das Berechtigungskonzept von SAP S/4HANA	399
10.1	Wechsel von SAP ERP zu SAP S/4HANA	399
10.1.1	Nicht mehr unterstützte Komponenten in SAP S/4HANA	400
10.1.2	Simplification List for SAP S/4HANA	402
10.1.3	SAP Fiori Apps Reference Library	408
10.1.4	Empfehlungen für SAP-Fiori-Apps in der SAP Fiori Apps Reference Library	411
10.1.5	Manuelle Auswertungen zu nutzbaren SAP-Fiori-Apps	415
10.2	Technische Sicherheit in SAP S/4HANA	418
10.3	Berechtigungen zur Ausführung von SAP-Fiori-Apps	423
10.3.1	Berechtigungen für das SAP Fiori Launchpad	423
10.3.2	Berechtigungen auf dem Frontend-Server	427
10.3.3	Berechtigungen auf dem Backend-Server	430
10.3.4	Auswertung von Apps in Rollen	432
11	Auditing in SAP HANA	437
11.1	Konfiguration des Auditings in SAP HANA	437
11.1.1	Systemparameter zur Auditing-Konfiguration	437
11.1.2	Konfiguration in Multi-Tenant-Systemen	441
11.1.3	Pflege der Auditing-Konfiguration mit dem SAP HANA Cockpit	442
11.1.4	Pflege der Auditing-Konfiguration mit dem SAP HANA Studio	444
11.1.5	Pflege der Auditing-Konfiguration mit SQL	445

11.2 Einrichten von Policies	446
11.2.1 Beispiele für Policies	452
11.2.2 Automatisch protokollierte Aktionen	454
11.2.3 Einrichten von Policies mit dem SAP HANA Cockpit	455
11.2.4 Einrichten von Policies mit dem SAP HANA Studio	460
11.2.5 Einrichten von Policies mit SQL	463
11.2.6 Speicherung der Policies in der Datenbank	465
11.2.7 Das Skript HANA_Security_AuditPolicies	466
11.3 Auswertung des Auditings	468
11.3.1 Die Views AUDIT_LOG und ALL_AUDIT_LOG	468
11.3.2 Konzept zur Auswertung	471
11.3.3 Auswertung des Auditings mit dem SAP HANA Cockpit	472
11.3.4 Auswertung des Auditings mit SQL	475
11.3.5 Auswertung des Auditings im UNIX SysLog	476
11.4 Löschen von Auditing-Protokollen	477
11.5 Auditing in SAP HANA XSA	479
11.5.1 Protokollierung im SAP HANA XSA Cockpit	479
11.5.2 Protokollierung in SAP-HANA-XSA-Anwendungen	481
11.6 Best-Practice-Empfehlungen	484
11.6.1 Pflege von Benutzern	485
11.6.2 Pflege von Katalog- und HDI-Rollen	486
11.6.3 Zuordnung von Rollen und Berechtigungen	487
11.6.4 Anmeldungen von Benutzern zu ungewöhnlichen Zeiten	488
11.6.5 Ändern von Systemparametern	488
11.6.6 Protokollierung von Aktionen des Benutzers SYSTEM	489
11.6.7 Protokollierung von Aktionen des Notfallbenutzers	489
11.6.8 Ausführung von DDL-Befehlen im Produktivsystem	490
11.6.9 Ändern der Einstellung der Verschlüsselung	491
11.6.10 Anschluss neuer Systeme zur Authentifizierung	492
11.6.11 Einspielen und Löschen von Lizenzen	493
11.6.12 Pflege von Remote Sources	493
11.6.13 Importieren und Aktivieren von Repository-Content	494
11.6.14 Zugriff auf Daten von SAP ERP/SAP S/4HANA	495
11.6.15 Versuch des Zugriffs auf Daten von SAP ERP bzw. SAP S/4HANA	496
11.6.16 Löschen von Tenant-Datenbanken	496
11.6.17 Pflege von Tenant-Datenbanken	497
11.6.18 Stoppen von Tenant-Datenbanken	497

12	Checklisten zur Analyse der Sicherheit von SAP HANA	499
<hr/>		
12.1	Einführung in SAP HANA	499
12.1.1	Der technische Aufbau von SAP HANA	499
12.1.2	SAP HANA Cockpit	500
12.1.3	DBA Cockpit	501
12.1.4	SAP HANA XS Advanced	503
12.1.5	SAP HANA und SAP ERP bzw. SAP S/4HANA	504
12.2	Netzwerk- und Betriebssystemsicherheit	505
12.2.1	Absicherung der UNIX-Benutzer	505
12.2.2	Schutz von Dateien und Verzeichnissen	506
12.2.3	Schutz von exportierten Dateien	507
12.2.4	Zugriff auf die UNIX-Ebene vom ABAP-Stack aus	507
12.2.5	Protokollierung von Aktionen unter UNIX	509
12.3	Systemsicherheit in SAP HANA	509
12.3.1	Verwaltung von Lizenzen	509
12.3.2	Pflege von Systemparametern	511
12.3.3	Verschlüsselung von Daten	513
12.3.4	Verschlüsselung der Kommunikation	515
12.3.5	Verbindungen zu anderen Systemen – Remote Sources	516
12.3.6	Alerts	519
12.4	Sicherheit in Multi-Tenant-Datenbanken	520
12.4.1	Das Konzept der Tenant-Datenbanken	520
12.4.2	Tenant-übergreifende Zugriffe	521
12.4.3	Nicht änderbare Parameter in Tenants	521
12.4.4	Einschränkung von Funktionen in Tenants	522
12.4.5	High Isolation Level für Tenants	522
12.4.6	Protokollierung von Änderungen an Tenants	523
12.5	Authentifizierung in SAP HANA	523
12.5.1	Authentifizierungsmethoden	523
12.5.2	Kennwortrichtlinien	525
12.6	Benutzerverwaltung in SAP HANA	527
12.6.1	Der Benutzerstammsatz	527
12.6.2	SAP HANA XS Advanced-Benutzer	529
12.6.3	SAP-HANA-Standardbenutzer	530
12.6.4	Benutzergruppen	531

12.7	Das Berechtigungskonzept von SAP HANA	532
12.7.1	Das Konzept der SAP-HANA-Berechtigungen	532
12.7.2	System Privileges	532
12.7.3	Object Privileges	533
12.7.4	Package Privileges	534
12.7.5	Analytic Privileges	535
12.7.6	Direkte Zuordnung von Privileges	535
12.7.7	Berechtigungen in SAP HANA XS Advanced	536
12.8	Das Rollenkonzept von SAP HANA	537
12.8.1	Eigenschaften von Rollen	537
12.8.2	Runtime-Katalogrollen	538
12.8.3	Design-Time-Repository-Rollen (XSC)	538
12.8.4	Design-Time-HANA-DI-Rollen (XSA)	540
12.8.5	SAP-HANA-Standardrollen	542
12.9	Analyse des SAP-HANA-Berechtigungskonzepts	543
12.10	Das Berechtigungskonzept von SAP S/4HANA	544
12.11	Auditing in SAP HANA	547
12.11.1	Konfiguration des Auditings in SAP HANA	547
12.11.2	Einrichten von Policies	548
12.11.3	Auswertung des Auditings	550
12.11.4	Löschen von Auditing-Protokollen	550
12.11.5	Auditing in SAP HANA XSA	551
Anhang		553
A	Sicherheitsrelevante Systemparameter	555
B	Sicherheitsrelevante Views in SAP HANA	559
C	Sicherheitsrelevante Tabellen in SAP S/4HANA	563
D	Der Autor	567
Index		569